

EXHIBIT A

Original

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

20 MAG 3878

TO BE FILED UNDER SEAL

**Agent Affidavit in Support of
Application for Search and Seizure
Warrant**

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for: (1) a black/dark grey OnePlus cell phone seized from Ruben Weigand on or about March 9, 2020; (2) a silver MacBook Pro Model A1502 bearing serial number C02RP1LJFVH8 seized from Ruben Weigand on or about March 9, 2020; and (3) a black/dark grey Apple iPhone seized from Ruben Weigand on or about March 9, 2020. [USAO Ref. No. 2020R00321](#)

SOUTHERN DISTRICT OF NEW YORK) ss.:

Matthew Mahaffey, a Special Agent with the Federal Bureau of Investigation, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office and I have been employed in this position since November 2016. During that time, I have participated in investigations of securities and wire fraud, bank fraud, and money laundering, and, among other things, have conducted or participated in surveillance, debriefings of witnesses, reviews of taped conversations and financial records, and the execution of search warrants. In particular, and as relevant to this application, I have participated in the execution of search warrants involving physical premises, electronic devices, and other electronic evidence.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices specified below (the "Subject Devices") for the items and information described in Attachment A. This affidavit is

based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (ESI). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Devices

3. The Subject Devices are particularly described as follows:

a. A black/dark grey OnePlus cell phone seized from Ruben Weigand on or about March 9, 2020 (Subject Device-1). Subject Device-1 is depicted below:



b. A silver MacBook Pro Model A1502 bearing serial number C02RP1LJFVH8 seized from Ruben Weigand on or about March 9, 2020 ([Subject Device-2]]. Subject Device-2 is depicted below:



c. A black/dark grey Apple iPhone seized from Ruben Weigand on or about March 9, 2020. ([Subject Device-3,]and together with Subject Devices -1 and -2, the [Subject Devices]]. Subject Device-3 is depicted below:



4. Based on my training, experience, and research, I know that the Subject Devices have capabilities that allow them to serve as devices through which users can conduct voice calls, and can be used as digital cameras, portable media players, GPS navigation devices, and PDAs.

5. As described in further detail below, the Subject Devices were seized from Ruben Weigand ([Weigand] on or about March 9, 2020, at the Los Angeles International Airport ([LAX] in California.

6. The Subject Devices were transported from California to New York and arrived in the Southern District of New York on or about March 25, 2020. The Subject Devices are presently located in the Southern District of New York.

C. The Subject Offenses

7. For the reasons detailed below, I submit that there is probable cause to believe that the Subject Devices contain evidence, fruits, and instrumentalities of bank fraud, and money laundering, in violation of Title 18, United States Code, Sections 1344 (bank fraud), 1349 (conspiracy to commit bank fraud), 1956 (money laundering), 1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 1956(h) (conspiracy to commit money laundering) (the [Subject Offenses])

II. Probable Cause

A. Probable Cause Regarding Subjects [Commission of the Subject Offenses

Overview of the Transaction Laundering Scheme

8. On or about March 9, 2020, a grand jury empaneled in the Southern District of New York returned a superseding indictment, S3 20 Cr. 188 (JSR) (the [Indictment], charging Weigand and Hamid Akhavan, a/k/a [Ray Akhavan] ([Akhavan], with one count of violating Title 18, United States Code, Section 1349 (conspiracy to commit bank fraud), from in or around 2016, through at least in or around 2019. A copy of the Indictment is attached hereto as Exhibit 1

and incorporated herein by reference. Weigand was arrested later that same day, March 9, 2020, at LAX, and the Subject Devices were seized from Weigand at the time of his arrest.

9. As set forth in greater detail in the Indictment, Weigand and Akhavan, working with others, including principals from [REDACTED], one of the leading on-demand marijuana delivery companies in the United States, planned and executed a scheme to deceive United States banks and other financial institutions into processing over one hundred million dollars in credit and debit card payments for the purchase and delivery of marijuana products (the "Transaction Laundering Scheme"). Because many United States banks are unwilling to process payments involving the purchase of marijuana, Weigand, Akhavan, and others used fraudulent methods so that [REDACTED] could avoid these restrictions and receive tens of millions of dollars from its customers, primarily located in California and Oregon who purchased marijuana products through the company. (Indictment ¶ 1). At least some of the banks and other financial institutions victimized by this criminal activity are located in the Southern District of New York.

10. As further set forth in the Indictment, [REDACTED] operated a technology platform that enabled customers to place online orders for various marijuana products offered by different dispensaries listed on [REDACTED] website and mobile application (collectively, the "Applications"). As a result of the Transaction Laundering Scheme, at various times between 2016 and 2019, [REDACTED] was able to offer its customers the ability to pay for purchases of marijuana products with credit and debit cards. (*Id.* ¶ 4). Once a customer placed an order, a delivery driver arranged by the dispensary would deliver the order to the customer shortly thereafter. Once the delivery was complete, [REDACTED] would generate and transmit via email a receipt for the purchase. (*Id.* ¶ 5). The fact that the transaction involved the purchase of marijuana, however, was concealed from the

bank or financial institution responsible for approving the payment —that is, the cardholder’s issuing bank —which otherwise would have declined the transaction. (*Id.* ¶¶ 2, 8-9).

11. To effectuate the Transaction Laundering Scheme, Weigand, Akhavan, and several of the principals of [REDACTED], including the company’s CEO, arranged for the money received from [REDACTED]’s customers to be disguised as payments to over a dozen phony online merchants and other non-marijuana businesses (the “Phony Merchants”), including transactions that appeared to be for stenographic services, music stores/pianos, and cosmetic stores.¹ Weigand, Akhavan, and others, worked with other co-conspirators to create at least a dozen Phony Merchants. The Phony Merchants also typically had web pages that suggested that they were involved in selling legitimate goods, such as carbonated drinks, face cream, dog products, and diving gear. For example, images that were displayed on a website for one of the Phony Merchants that purportedly sold carbonated water products is shown below:

¹ A list of several of the website names associated with the Phony Merchants appears in paragraph 13 of the Indictment. Based on my participation in this investigation and my review of electronic communications involving Weigand, Akhavan and other co-conspirators, I learned that additional website names associated with the Phony Merchants included organikals.store, greendenvale, mentaldossier.com, indus-distr.com, osteofiles.com, goodgreenbazaar.com, medical-stf.com, and medical-dsr.com. Based on my participation in this investigation and my review of electronic communications involving Weigand, Akhavan and other co-conspirators, I also learned that the Phony Merchants involved in the scheme included Lorry Ltd., Linebeck, Hot Robots, International Standard, and New Opal Ltd.



12. To accomplish this deceptive scheme, ██████ relied on third party payment processors (the Payment Processors) who worked with Weigand, Akhavan, and other co-conspirators to create phony offshore corporations and websites (*i.e.*, the Phony Merchants) and open offshore merchant bank accounts. As set forth in more detail below, one of Weigand's responsibilities was to submit applications on behalf of the Phony Merchants to these offshore banks in order to open merchant bank accounts for the Phony Merchants. Weigand, Akhavan and other members of the conspiracy then used the Phony Merchants' offshore bank accounts to disguise payments made to ██████ for the purchase of marijuana products, thereby deceiving United States banks about the true nature of the financial transactions they were processing. Working together, Weigand, Akhavan, other Payment Processors, and principals of ██████ deceived United States banks and financial institutions—including federally insured institutions—into processing tens of millions of dollars in marijuana purchases made through ██████. (*Id.* ¶ 2; *see also id.* ¶¶ 8, 12-14). According to my review of bank records and other evidence gathered in the investigation, and as set forth in the Indictment, the Transaction Laundering Scheme generated more than approximately \$100 million in credit and debit card transactions. (*Id.* ¶ 14). Based on evidence

obtained to date, it appears that [REDACTED] stopped processing credit card transactions in approximately mid-2019.

13. Among other sources of information in this investigation is information provided by a cooperating witness (CW-1)² with whom Akhavan contracted to receive services to implement the Transaction Laundering Scheme. According to CW-1, as corroborated by other evidence, among other roles CW-1 played in the charged conspiracy, CW-1 assisted Weigand, Akhavan, and other co-conspirators in the creation and development of the Phony Merchants and phony merchant websites and the preparation of associated fraudulent merchant applications, agreements, and related documents to submit to banks and financial institutions. CW-1 provided documents to the Government corroborating CW-1's statements regarding these activities, and agents have obtained additional recordings, electronic communications, financial records, and other evidence corroborating CW-1's statements.

14. From information provided by CW-1, and from my review of financial records, information provided by representatives of [REDACTED],³ and a representative of a marijuana dispensary with which [REDACTED] contracted, I have learned that credit and debit payments received by [REDACTED] in exchange for marijuana products were typically processed and settled through one or more payment processors located outside the United States, and the payments were then typically sent

² CW-1 has pleaded guilty to conspiring to commit bank fraud, conspiring to commit money laundering, and Hobbs Act extortion offenses pursuant to a cooperation agreement with the United States Attorney's Office for the Southern District of New York. In connection with CW-1's assistance, CW-1 has provided information and records to law enforcement, and hopes to receive leniency at sentencing. Information provided by CW-1 has been corroborated, in part, by recordings, electronic communications, and other records.

³ [REDACTED], through counsel, is voluntarily cooperating with this investigation in hopes of receiving leniency for the company.

by international wire back into the United States to accounts controlled by the marijuana dispensaries.

B. Probable Cause Justifying Search of the Subject Devices

15. As noted above, the Subject Devices were seized from Weigand on or about March 9, 2020, when Weigand was arrested at LAX. The Subject Devices have been maintained in FBI custody since that time, and transported to the Southern District of New York, where they arrived on or about March 25, 2020.

16. Based on my participation in this investigation, and my review of phone messages and emails, I have learned that Weigand, Akhavan, and other co-conspirators, frequently appear to have used electronic devices such as cell phones and computers to send and receive communications in furtherance of the Transaction Laundering Scheme. For example, as set forth below, Weigand, Akhavan, and other co-conspirators communicated through the use of a messaging application for cell phones, tablets, and computers, through which users can send and receive end-to-end encrypted⁴ messages (the Encrypted Messaging Application). Furthermore, Weigand, Akhavan, and other co-conspirators also communicated through the use of an end-to-

⁴ End-to-end encryption is a system of communication where only the communicating users can read the messages. End-to-end encryption prevents third parties —including law enforcement — from being able to access the cryptographic keys needed to decrypt the conversation. This means that law enforcement agents are unable to intercept or —wiretap —communications that are sent through end-to-end encryption, and, furthermore, are unable to view the content of such communications through the use of search warrants that are served on the service providers. However, such communications can be stored on a cell phone, tablet, laptop, or other similar electronic devices, and accessed through a search of those devices, such as the searches the Government seeks authorization to conduct here. Indeed, some of the encrypted messages referenced in this affidavit were obtained from the cellphone of CW-1 after he was arrested and began cooperating with law enforcement.

end encrypted email service based in Switzerland (the "Encrypted Email Service").⁵ Based on my training, experience, and participation in this investigation, I have learned that individuals who are engaged in criminal activity frequently use end-to-end encrypted communication services such as the Encrypted Messaging Application and the Encrypted Email Service in an effort to evade detection by law enforcement (e.g., by preventing law enforcement agents from collecting incriminating evidence through methods such as wiretaps and search warrants).

17. Based on my review of messages that were sent and received through the Encrypted Messaging Application, I have learned that Weigand, Akhavan, and other co-conspirators participated in several group chats in which they communicated about the Transaction Laundering Scheme. For example, the following messages were sent and received through the Encrypted Messaging Application in a group chat in which Weigand and Akhavan were participants:

a. On or about April 27, 2018, participants in a group chat that included CW-1, Weigand, and Akhavan, sent a series of messages through the Encrypted Messaging Application about the Transaction Laundering Scheme.⁶ In particular, the following messages were sent and received on or about April 27, 2018:

Akhavan: When do you think they can go online?

CW-1: Monday[.] I will have them ready for Ruben [Weigand] in the morning.

Akhavan: [CW-1]. Add a 2 dollar option somewhere please[.] The lowest two charges are 2 and 5[.]

Weigand: Do you really think 2 makes sense? I think I wouldn't allow below 10[.]

CW-1: Ok

⁵ Based on my review of public source material, and my participation in this investigation, I have learned that users can send and receive emails through the Encrypted Email Service using cell phones, tablets, and computers.

⁶ Two of the participants in this chat have the display names "Ray CE" and "Ruben Weigand." Based on my conversations with CW-1, I have learned the "Ray CE" refers to Akhavan and "Ruben Weigand," refers to Weigand.

Akhavan: Yea but its not up to what we allow[.] [I]t s[up] to the products [REDACTED] sells[.] [T]hose are the prices th[er]e[sic] gonna see.

Based on my training, experience, participation in this investigation, and conversations with CW-1, I believe that in the beginning of this message exchange, Weigand, Akhavan, and CW-1, are discussing the timeline for when a particular website or websites for one or more of the Phony Merchants were going to become available for processing credit and debit card marijuana purchases for [REDACTED] customers (Akhavan: ¶When do you think they can go online? ¶CW-1: ¶Monday[.] I will have them ready for [Weigand] in the morning. ¶) Furthermore, in the remainder of this message exchange, it appears that Weigand, Akhavan, and CW-1, are discussing what is sometimes referred to in other similar communications as the ¶price point ¶issue. Based on my participation in this investigation, I have learned that the price point issue refers to efforts by Weigand, Akhavan, and others, to ensure that the prices for the products that were displayed on the websites for the Phony Merchants were consistent with the prices for the products that were being sold through [REDACTED] s[up]Applications. Here, in this message exchange, Akhavan appears to be informing Weigand that the websites for the Phony Merchants need to include a product with a purchase price of \$2, in order to match the price of the least expensive product being offered by [REDACTED]. Based on my training, experience, participation in this investigation, and conversations with CW-1, I have learned that matching the price points was particularly important in order for the co-conspirators to avoid unwanted scrutiny by banks and credit card companies. For example, if a credit card company or bank checked the website for a Phony Merchant, and the prices on that website did not match up with the prices on the [REDACTED] customers ¶bank statements, this would be a red flag that the Phony Merchant websites were not legitimate.

b. On that same day, April 27, 2018, Weigand and CW-1 exchanged additional group chat messages through the Messaging Application about the Transaction Laundering Scheme. In particular, the following messages were sent and received on or about April 27, 2018:

CW-1: Hot Robot application pack is ready minus bank reference letter & iban details. [REDACTED] informed us we will have them Monday morning.

Weigand: Let [REDACTED] submit Monday morning in that case [REDACTED] if you want send through for review. Have you been able to obtain better quality scans.

CW-1 Ok. Yes.

Weigand Cool.

As noted above, Hot Robots was one of the Phony Merchants that was used during the Transaction Laundering Scheme. In this message exchange, it appears that Weigand and CW-1 are discussing the submission of a merchant account application to a bank on behalf of a Phony Merchant. In particular, it appears that CW-1 is informing Weigand that the merchant application package was ready for submission, and in response Weigand told CW-1 that they should submit the application on Monday morning and that Weigand could review the application before it was submitted. Based on my conversations with CW-1, and my review of encrypted electronic communications, *see, e.g.,* ¶ 18(a), I have learned, among other things, that one of Weigand's responsibilities in the Transaction Laundering Scheme was to find European banks that members of the Transaction Laundering Scheme could use to open bank accounts for the Phony Merchants and process [REDACTED]'s marijuana transactions.

c. On or about April 27, 2018, participants in a group chat that included Weigand, Akhavan, and CW-1, sent a series of additional messages through the Messaging Application about the Transaction Laundering Scheme. In particular, the following messages were sent and received on or about April 27, 2018:

Akhavan: [CW-1,] Ruben [Weigand] is asking about descriptors

Weigand: We we discussed it, just need u to confirm. [M]edical-stf.com / 877-975-5510. [M]edical-dsr.com / 877-974-7750.

CW-1: We acquired the domain for these 2 and the 2 ray [Akhavan] picked from the list I sent, just let us know which ones you want in the end

Weigand: [M]edical-stf.com / 877-975-5510. [M]edical-dsr.com / 877-974-7750. They are set up at the bank.

Based on my training, experience, participation in this investigation, and conversations with CW-1, it appears that in this message exchange, Weigand, Akhavan, and CW-1, are discussing the descriptors⁷ that are going to be used for the purchases of marijuana through [REDACTED] technology platform. Notably, these descriptors did not make any reference to [REDACTED], which was the actual company from which the customers made their purchases; instead, the descriptors referenced [REDACTED]medical-stf.com [REDACTED] and [REDACTED]medical-dsr.com. [REDACTED]⁸ In addition, in this message exchange, Weigand refers to descriptors that included what appear to be 877 [REDACTED] customer service phone numbers. Based on my review of additional messages sent and received by Weigand, Akhavan, and other co-conspirators, and my conversations with CW-1, I learned that members of the Transaction Laundering Scheme included customer service numbers in the descriptors so that [REDACTED] customers would not be confused about the descriptors on their credit card statements. In particular, because [REDACTED] marijuana customers were making purchases from [REDACTED], through its Applications, and not [REDACTED]medical-stf.com [REDACTED] or [REDACTED]medical-dsr.com, [REDACTED] Weigand, Akhavan, and other members of the conspiracy took steps to ensure that if those customers were confused by the descriptors on their credit card statements, they could figure out that the purchases were for [REDACTED] products by calling

⁷ Descriptor commonly refers to the short description of the goods or services that were purchased with a credit or debit card that appears on the card statement for the issuing bank and is used to identify the merchant with whom each transaction on the statement took place. Descriptors also often include a reference to the name of the merchant from whom the customer purchased a particular product from (e.g., a purchase from Amazon would include a reference to [REDACTED]amazon [REDACTED] in the descriptor).

⁸ The descriptors also did not make any reference to the purchase of marijuana products.

one of the 877 customer service numbers listed in the descriptors. Once the customers called those numbers, and verified that they were legitimate [REDACTED] customers, the customer service agents would inform them that the transactions listed on their statements were for the purchase of [REDACTED] products.

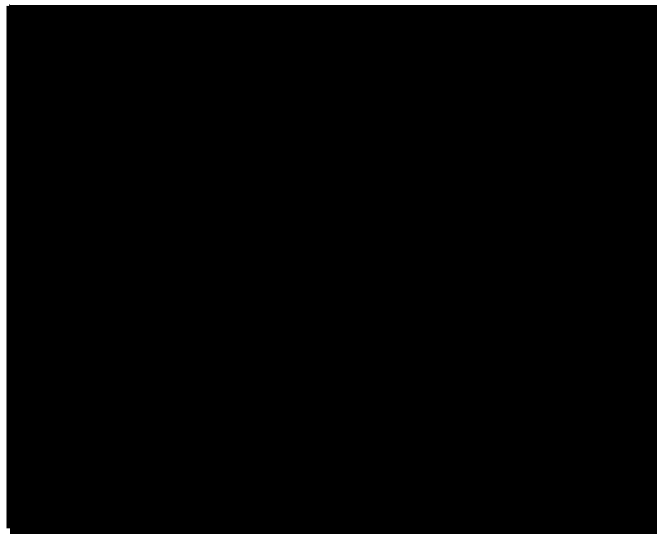
18. Based on my review of messages that were sent and received on the Messaging Application, I have learned that Weigand, Akhavan, and other co-conspirators participated in another group chat in which they communicated with several employees at [REDACTED], including [REDACTED] former CEO, about the Transaction Laundering Scheme (the [REDACTED] Group Chat). Based on my review of those messages I have learned the following, among other things:

a. On or about July 31, 2018, Weigand, and another co-conspirator not named herein (CC-1), received an electronic chat invitation from Akhavan and joined the [REDACTED] Group Chat. After Weigand and CC-1 joined the [REDACTED] Group Chat, Akhavan sent a message to the group stating, "Good morning team [REDACTED]." Akhavan went on to write, "I've added [CC-1] and Ruben . . . Have good news . . . [CC-1] and Ruben have both agreed to be actively involved with helping us out. [CC-1] is handling all reporting and reconciliation. And Ruben is interfacing with the banks. You all met Ruben in L.A. and [CC-1] will be out soon hopefully as well."

b. In that same chat, Akhavan went on to explain in substance and in part, that his team had two banks accounts that they had been using to process [REDACTED] transactions, and that the same bank had given them two additional accounts to use. Akhavan also noted that another bank "has given us 2 more accounts that were supposed to become operational that same day. In the same chat, Akhavan later stated, "How we route this and split this is important and I wanted to get you guys integrated with Ruben so you can work together to Route and back up each depot in the smartest way."

19. Based on my training, experience, participation in this investigation, and conversations with CW-1, I have learned the following, among other things, about a meeting that took place in Calabasas, California, during which Weigand, CW-1, and Akhavan, among others, discussed the Transaction Laundering Scheme:

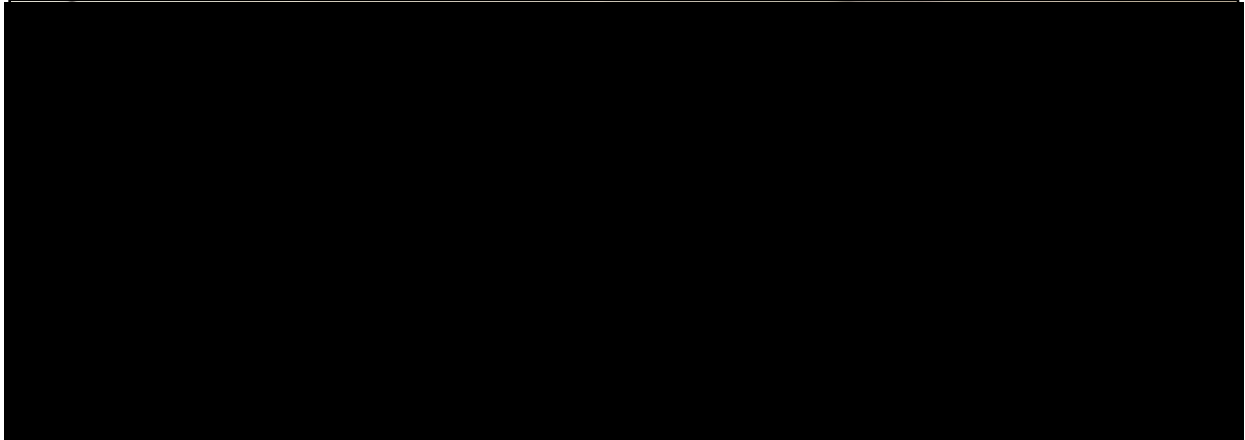
a. Based on my conversations with CW-1, I have learned that on or about January 17, 2018, co-conspirators in the Transaction Laundering Scheme met in Calabasas, California, for a meeting to discuss the Transaction Laundering Scheme (the Meeting). Weigand, Akhavan, CW-1, and others, were present at the Meeting. A photograph that was taken at the Meeting by CW-1 is depicted below. Weigand is the individual depicted on the left side of the photograph, holding what appears to be a cell phone in his hand.⁹



b. During the Meeting, the co-conspirators discussed, among other things, operational details regarding how the Transaction Laundering Scheme would work. Specifically, among other things, attendees at the meeting discussed that the underlying transactions that were going to be processed through the Phony Merchants were for the company [REDACTED]. Furthermore, the

⁹ Based on my review of the metadata associated with this image, and the image shown below, I have learned that both images are dated January 17, 2018.

attendees at the meeting discussed the details of how the payment processing would work, including the use of Phony Merchants with overseas bank accounts. During the meeting, some of the attendees at the meeting, including but not limited to Akhavan, drew a diagram on a white board that depicted how the Transaction Laundering Scheme was intended to work. CW-1 took a picture of that diagram, which is shown below:



c. Based on my review of travel records for Weigand, I have learned that Weigand traveled from Munich, Germany, to Los Angeles, California, on or about January 15, 2018, and flew back to Zurich, Switzerland on or about January 29, 2018, from Los Angeles, California. Furthermore, based on my review of travel records for CW-1, I have also learned that CW-1 arrived in Los Angeles, California, from Europe, on or about January 14, 2018, and flew out of the United States on or about January 18, 2018.

20. Based on my review of messages that were sent and received on the Messaging Application, it appears that Weigand, Akhavan, and other co-conspirators sent and received messages on the Messaging Application regarding the Transaction Laundering Scheme at least as recently as late-2018. Furthermore, based on my review of email communications sent and received through the Encrypted Email Service, I have learned, among other things, that co-

conspirators in the Transaction Laundering Scheme sent and received emails in which they discussed the Transaction Laundering Scheme as recently as May 2019.

21. Based on my conversations with CW-1, and my review of a recording of a phone call between CW-1 and Weigand, I know that Weigand and CW-1 communicated by telephone as recently as in or around May 2019. During that conversation, Weigand stated, in substance and in part, that he remained involved with the processing of payments on behalf of [REDACTED].

22. Like individuals engaged in any other kind of activity, individuals who engage in fraud and money laundering offenses store records relating to their illegal activity and to persons involved with them in that activity on electronic devices such as the Subject Devices. Such records can include, for example, logs of electronic chats with co-conspirators, such as the chats described above; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts; photographs of co-conspirators; location evidence revealing the user's location at relevant times; and/or records related to financial transactions involving criminal proceeds, including records pertaining to entities, bank accounts, and individuals involved in such transactions. Individuals engaged in criminal activity often store such records in order to, among other things, (1) keep track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; and (3) keep an accounting of illegal proceeds for purposes of, among other things, dividing those proceeds with co-conspirators.

23. Computer files or remnants of such files can be recovered months or even years after they have been created or saved on electronic devices such as the Subject Devices. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Thus, the ability to retrieve

information from the Subject Devices depends less on when the information was first created or saved than on a particular user's device configuration, storage capacity, and computer habits.

24. Based on the foregoing, I respectfully submit there is probable cause to believe that Weigand, Akhavan, and other co-conspirators are engaged in the bank fraud and money laundering offenses described above, and that evidence of this criminal activity is likely to be found on the Subject Devices. In particular, I believe that the Subject Devices are likely to contain the following information:

- a. Evidence concerning the identity or location of the owner or user of the Subject Devices;
- b. Evidence concerning the identity or location of, and communications with, suspects, co-conspirators, and/or victims of the Subject Offenses, including but not limited to IP address information, communications, photos, videos, or other attachments, and address book information, covering the time period of 2016 to 2019;
- c. Evidence of the Subject Offenses, such as communications, contact lists and address books, videos, images, and other stored content information presently contained in, or on behalf of, the Subject Devices, covering the time period of 2016 to 2019;
- d. Evidence of the relationships between suspects, co-conspirators, and/or victims involved in the Subject Offenses, covering the time period of 2016 to 2019;
- e. Evidence concerning financial transactions conducted by or between the co-conspirators and/or victims of the Subject Offenses, including but not limited to the dates and amounts of such transactions, the identity of and other identifying information for the parties to such transactions and any entities involved in such transactions, and the bank account and accountholder information for any bank accounts used in such transactions, covering the time period of 2016 to 2019;
- f. Evidence concerning the location of other evidence of the Subject Offenses, including but not limited to information concerning email or other social media accounts potentially containing relevant evidence;
- g. Passwords or other information needed to access a user's electronic device(s) or other online accounts that may contain evidence of the Subject Offenses;
- h. Non-content transactional information of activity of the Subject Devices, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations; and

i. Subscriber information, in any form kept, pertaining to the Subject Devices, including, but not limited to, applications, subscribers' full names, all user names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records.

III. Procedures for Searching ESI

A. Review of ESI

25. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the Subject Devices for information responsive to the warrant.

26. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- ☐* surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- ☐* conducting a file-by-file review by ☐opening ☐or reading the first few ☐pages ☐of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- ☐* ☐scanning ☐storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and
- ☐* performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

27. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Devices to locate all data responsive to the warrant.

B. Return of the Subject Devices


28. If the Government determines that the Subject Devices are no longer necessary to retrieve and preserve the data on the devices, and that the Subject Devices are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject Devices, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion

29. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

S/_____
Matthew Mahaffey
Special Agent
Federal Bureau of Investigation

Sworn to before me on
April 14, 2020



HONORABLE KATHARINE H. PARKER
United States Magistrate Judge
Southern District of New York

*sworn to before me by reliable electronic means
pursuant to Fed. R. Crim. P. 4.1

Original

Attachment A

I. Devices Subject to Search and Seizure

The devices that are the subject of this search and seizure warrant (the "Subject Devices") are described as follows:

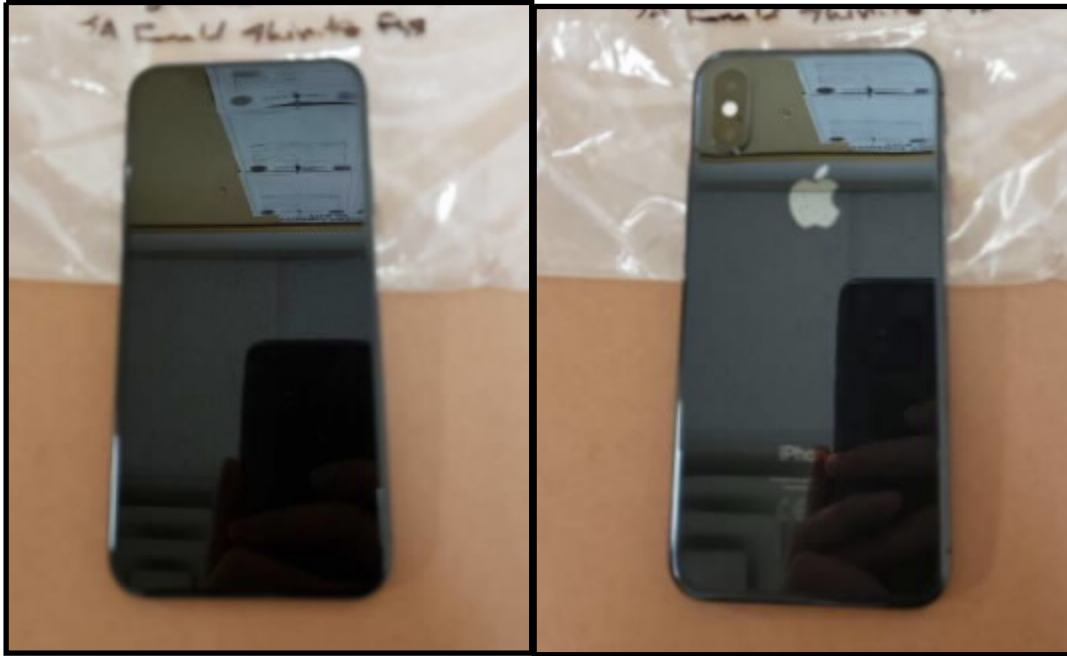
1. A black/dark grey OnePlus cell phone seized from Ruben Weigand on or about March 9, 2020 ("Subject Device-1"). Subject Device-1 is depicted below:



2. A silver MacBook Pro Model A1502 bearing serial number C02RP1LJFVH8 seized from Ruben Weigand on or about March 9, 2020 ("Subject Device-2"). Subject Device-2 is depicted below:



3. A black/dark grey Apple iPhone seized from Ruben Weigand on or about March 9, 2020 (Subject Device-3). Subject Device-3 is depicted below:



II. Review of ESI on the Subject Devices

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Devices for evidence, fruits, and instrumentalities of bank fraud, and money laundering, in violation of Title 18, United States Code, Sections 1344 (bank fraud), 1349 (conspiracy to commit bank fraud), 1956 (money laundering), 1957 (engaging in monetary transactions in property derived from specified unlawful activity), and 1956(h) (conspiracy to commit money laundering) (the Subject Offenses) described as follows:

1. Evidence concerning the identity or location of the owner or user of the Subject Devices;
2. Evidence concerning the identity or location of, and communications with, suspects, co-conspirators, and/or victims of the Subject Offenses, including but not limited to IP address information, communications, photos, videos, or other attachments, and address book information, covering the time period of 2016 to 2019;
3. Evidence of the Subject Offenses, such as communications, contact lists and address books, videos, images, and other stored content information presently contained in, or on behalf of, the Subject Devices, covering the time period of 2016 to 2019;

4. Evidence of the relationships between suspects, co-conspirators, and/or victims involved in the Subject Offenses, covering the time period of 2016 to 2019;

5. Evidence concerning financial transactions conducted by or between the co-conspirators and/or victims of the Subject Offenses, including but not limited to the dates and amounts of such transactions, the identity of and other identifying information for the parties to such transactions and any entities involved in such transactions, and the bank account and accountholder information for any bank accounts used in such transactions, covering the time period of 2016 to 2019;

6. Evidence concerning the location of other evidence of the Subject Offenses, including but not limited to information concerning email or other social media accounts potentially containing relevant evidence;

7. Passwords or other information needed to access a user's electronic device(s) or other online accounts that may contain evidence of the Subject Offenses;

8. Non-content transactional information of activity of the Subject Devices, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations; and

9. Subscriber information, in any form kept, pertaining to the Subject Devices, including, but not limited to, applications, subscribers' full names, all user names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records.

EXHIBIT 1

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - - X

UNITED STATES OF AMERICA

- v. -

HAMID AKHAVAN,
a/k/a "Ray Akhavan," and
RUBEN WEIGAND,

Defendants.

- - - - - X

:
:
: SEALED INDICTMENT

: S3 20 Cr. 188 ()

COUNT ONE

(Conspiracy to Commit Bank Fraud)

The Grand Jury charges:

OVERVIEW OF THE SCHEME

1. From at least in or about 2016, up to and including in or about 2019, HAMID AKHAVAN, a/k/a "Ray Akhavan," and RUBEN WEIGAND, the defendants, principals at one of the leading on-demand marijuana delivery companies in the United States (the "Online Marijuana Marketplace Company"), and other co-conspirators, engaged in a scheme to deceive United States banks and other financial institutions into processing in excess of one hundred million dollars in credit and debit card payments for the purchase and delivery of marijuana products (the "Transaction Laundering Scheme"). Because many United States banks are unwilling to process payments involving the purchase

of marijuana, the Online Marijuana Marketplace Company used fraudulent methods to avoid these restrictions and to receive in excess of one hundred million dollars from customers located in California and Oregon who purchased marijuana through the Online Marijuana Marketplace Company.

2. To effectuate the Transaction Laundering Scheme, HAMID AKHAVAN, a/k/a "Ray Akhavan," and RUBEN WEIGAND, the defendants, and several of the principals of the Online Marijuana Marketplace Company, arranged for the money received from the Online Marijuana Marketplace Company's customers to be disguised as payments to over a dozen phony online merchants and other non-marijuana businesses (the "Phony Merchants"), including transactions that appeared to be for stenographic services, music stores/pianos, and cosmetic stores. To accomplish this deceit, the Online Marijuana Marketplace Company relied on third party payment processors (the "Payment Processors") who worked with AKHAVAN, WEIGAND, and other co-conspirators to create phony offshore corporations and websites (i.e., the Phony Merchants) and open offshore merchant bank accounts. AKHAVAN, WEIGAND, and other members of the conspiracy used the Phony Merchants' offshore bank accounts to disguise payments made to the Online Marijuana Marketplace Company for the purchase of marijuana products and to deceive United States banks about the true nature of the financial transactions they were processing.

Working together, AKHAVAN, WEIGAND, other Payment Processors, and principals of the Online Marijuana Marketplace Company deceived United States banks and financial institutions—including federally insured institutions—into processing in excess of one hundred million dollars in marijuana purchases made through the Online Marijuana Marketplace Company.

BACKGROUND ON THE ONLINE MARIJUANA MARKETPLACE COMPANY

3. At all times relevant to this Indictment, the Online Marijuana Marketplace Company was a California-based company that arranged for on-demand sale and delivery of marijuana products to customers located in California and Oregon. Through the Online Marijuana Marketplace Company's mobile application and website (collectively, the "Applications"), customers could order marijuana from different dispensaries listed on the Applications. Specifically, customers used the Applications to select the marijuana product(s) of their choice, and to receive delivery of their selection shortly thereafter. Although the Online Marijuana Marketplace Company operated the technology platform through which users purchase marijuana (i.e., the Applications), it was not the actual retailer of the marijuana. The actual retailers, referred to as "dispensaries," contracted with the Online Marijuana Marketplace Company to fulfill orders placed by customers through the Applications.

4. To request and receive a delivery of marijuana through the Applications, a user created an Online Marijuana Marketplace Company account through the company's website or mobile application. Once the customer selected his or her product(s) for purchase, the Application generated a check-out screen for the order where the customer could select a payment option. At various points from in or around 2016, through in or around 2019, one of the payment options offered by the Online Marijuana Marketplace Company for purchases of marijuana were credit cards and debit cards. For purchases with credit cards or debit cards, the Applications allowed customers to enter their card information and then complete the payment using that information.

5. Once a customer placed an order, a delivery driver would deliver the order to the customer shortly thereafter. Once the delivery was complete, the Online Marijuana Marketplace Company generated and transmitted via email a receipt for the purchase. When customers made purchases by credit cards or debit cards, those purchases would appear on the customers' card statements as though they were from merchants other than the Online Marijuana Marketplace Company (e.g., a merchant from whom the customer had not in fact purchased the marijuana).

6. The Online Marijuana Marketplace Company stopped accepting credit card payments in or around mid-2019.

BACKGROUND ON CREDIT AND DEBIT CARD PROCESSING

7. Credit and debit card transactions are usually processed through payment networks (the "Payment Networks"), run by entities such as MasterCard or Visa (the "Credit Card Companies"), that provide authorization, clearing and settlement services for credit and debit card transactions. Financial institutions, as members of these payment networks, can offer payment processing services directly to merchants, but more commonly partner with non-bank third parties – including payment processors, Independents Sales Organizations ("ISOs"), and Merchant Service Providers ("MSPs," collectively with ISOs and payment processors, the "Processors") – for such third parties to process payments on behalf of the sponsoring financial institutions. These processors are typically required to be registered with the Payment Networks.

8. Processors typically use Payment Networks set up by the Credit Card Companies. The Credit Card Companies have rules that prohibit their credit cards from being used for marijuana purchases. Violations of these rules can lead to penalties and ultimately to a merchant being terminated. Debit cards that are issued by banks often fall under the same rules because the Processors typically use the Credit Card Companies' Payment Networks.

9. When purchases are made with a credit or debit card, merchant category codes ("MCCs") are assigned to each transaction that are specific to the category of product or service being purchased. Because the Credit Card Companies do not support marijuana transactions, they do not have marijuana merchant codes. As a result, in order to process a marijuana transaction through a Credit Card Company, a false merchant code – i.e., a merchant code associated with a different product or product category – would have to be used. HAMID AKHAVAN, a/k/a "Ray Akhavan," and RUBEN WEIGAND, the defendants, and their co-conspirators, used merchant codes for other products – typically referred to as "miscoding" – in order to get around these rules.

10. Online credit card and debit card payment transactions typically consist of two steps: (1) an authorization; followed by (2) clearing and settlement. Card authorization for online purchases generally works as follows:

a. A cardholder (i.e., the individual making the purchase online) initiates a transaction by entering a credit or debit card number, card expiration date, and other security features required by the merchant, such as the Card Verification Value ("CVV") number or the cardholder's zip code.

b. The merchant uses its payment software or gateway¹ to transmit the cardholder's information and the details of the transaction, including the name and location of the merchant, the MCC, a description of the goods and services purchased (sometimes referred to as the "descriptor"), the amount of the transaction, and the transaction date, to its partner Processor (or directly to the merchant's bank, which is often referred to as the "acquiring bank").

c. The Processor captures the transaction information and routes it through a Payment Network to the cardholder's "issuing bank," as defined below, to be approved or declined.

d. The bank issuing the credit or debit card to the customer ("issuing bank") receives the transaction information from the Processor and responds by approving or declining the transaction. Issuing banks in the United States generally will not extend credit (i.e., approve) transactions that involve unlawful activity under federal law, such as the sale of marijuana.²

¹ A payment gateway is a technology used by merchants to accept debit or credit card purchases from customers. For online sales, this typically refers to the "checkout" portals used to enter credit card information or credentials.

² Although the personal use of marijuana has been legalized under state law in several states, including California and Oregon, marijuana is a Schedule I Controlled Substance under the

e. The issuing bank sends a response code back to the Processor, and that code reaches the merchant's payment gateway and is stored in a batch file pending settlement, which is described below.

f. If the merchant receives authorization, the issuing bank will place a hold for the amount of the purchase on the cardholder's account pending settlement.

g. Finally, the merchant typically provides the customer a receipt to complete the sale. This entire authorization process usually takes place within seconds.

h. In order to accept transactions on behalf of the Credit Card Companies, the acquiring bank must be a registered member of the Credit Card Companies.

11. Step two of the credit card and debit payment card process is clearing and settlement, which pertains to the recording of the movement of funds ("clearing"), and the actual flow of funds ("settlement"). Clearing and settlement generally works as follows:

a. During the clearing stage, the issuing bank posts to each cardholder's account the transaction information that it received from the merchant (or from the Processor after

Controlled Substances Act, and the possession, distribution, and use of marijuana is unlawful under federal statutes, including Title 21, United States Code Sections 841 and 844.

receiving it from the merchant), including the name of the merchant and the amount for each transaction. However, in the clearing stage, there is no exchange or transfer of funds.

b. The acquiring bank then credits the merchant's account and submits the transaction to the respective Credit Card Company's Payment Network for settlement.

c. In the settlement stage, the Credit Card Companies use their Payment Networks to forward each transaction to the appropriate issuing bank, which ordinarily will transfer funds for the approved transaction, less a fee.

d. The Credit Card Companies typically use their Payment Networks to pay the acquiring bank (and sometimes the Processor) its respective percentages from the remaining funds, after which the Processor pays the merchant an amount equal to the cardholder purchases, minus a fee charged to merchants for processing the debit and credit card transactions (i.e., the "merchant discount rate").

e. The final step is for the issuing bank to use the information it has received from each transaction to prepare monthly cardholder statements, which are distributed to cardholders. These statements typically identify each credit or debit card purchase made by the cardholder, the amount of the purchase, and the name associated with the merchant.

THE TRANSACTION LAUNDERING SCHEME

12. During the time period charged in this Indictment, because most banks in the United States were unwilling to process credit and debit card transactions involving marijuana, HAMID AKHAVAN, a/k/a "Ray Akhavan," and RUBEN WEIGAND, the defendants, and other members of the conspiracy, used several strategies to trick United States issuing banks into authorizing marijuana transactions for the Online Marijuana Marketplace Company. The primary method used by AKHAVAN, WEIGAND, and other co-conspirators, involved the creation and use of the Phony Merchants. These fraudulent companies were used to open offshore bank accounts with merchant acquiring banks and to initiate credit card charges for marijuana purchases made through the Online Marijuana Marketplace Company. Because of the high risk associated with processing transactions that involved unlawful activity (i.e., the sale of marijuana), employees at some of the acquiring banks charged high fees for the acquiring banks to process these transactions.

13. HAMID AKHAVAN, a/k/a "Ray Akhavan," and RUBEN WEIGAND, the defendants, worked with other co-conspirators to create the Phony Merchants – including phony online merchants purportedly selling dog products, dive gear, carbonated drinks, green tea, and face creams – and establish Visa and MasterCard merchant processing accounts with one or more offshore acquiring banks.

AKHAVAN, WEIGAND, and their co-conspirators arranged for more than a dozen Phony Merchants to be used by the Online Marijuana Marketplace Company. For example, some of the website names for the Phony Merchants included: absolutsoda.com; diverkingdom.com; fly2skyshop.com; goodegreenbazaar.com; greenteacha.com; happypuppybox.com; outdoormaxx.com; and soniclogistix.com. The Phony Merchants also typically had web pages suggesting that they were involved in selling legitimate goods, such as carbonated drinks, face cream, dog products, and diving gear. Yet, as noted above, these companies were actually being used to facilitate the approval and processing of marijuana transactions. Furthermore, the Phony Merchants were not based in the United States, and many of them had the same address listed as their company address. In addition, while these entities claimed to be based outside the United States, their customer service telephone numbers were American phone numbers.

14. Between at least in or about 2017 and at least in or about July 2019, more than approximately \$100 million in credit and debit card transactions were processed for several of the Phony Merchants that were being used by HAMID AKHAVAN, a/k/a "Ray Akhavan," and RUBEN WEIGAND, the defendants, and other co-conspirators, to process marijuana purchases involving the Online Marijuana Marketplace Company. Some of the merchant websites listed for those transactions include: greenteacha.com,

medical-stf.com, organikals.store, and soniclogistix.com. AKHAVAN, and others, also worked with and directed others to apply incorrect MCCs to the Online Marijuana Marketplace Company marijuana transactions in order to disguise the nature of those transactions and create the false appearance that the transactions were completely unrelated to marijuana. Some of the MCCs/categories listed for the transactions listed above included stenographic services, music stores/pianos, and cosmetic stores. None of the merchant website names listed for those transactions referred to the Online Marijuana Marketplace Company or to marijuana.

STATUTORY ALLEGATIONS

15. From at least in or about 2016, up to and including in or about 2019, in the Southern District of New York and elsewhere, HAMID AKHAVAN, a/k/a "Ray Akhavan," and RUBEN WEIGAND, the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit bank fraud, in violation of Title 18, United States Code, Section 1344.

16. It was a part and object of the conspiracy that HAMID AKHAVAN, a/k/a "Ray Akhavan," and RUBEN WEIGAND, the defendants, and others known and unknown, willfully and knowingly, would and did execute, and attempt to execute, a scheme and artifice to defraud a financial institution, the deposits of which were then

federally insured, and to obtain moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, such financial institution, by means of false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344, to wit, AKHAVAN and WEIGAND participated in a scheme to deceive financial institutions and other financial intermediaries—including federally insured banks—into processing and authorizing payments to and from marijuana sale and delivery businesses and their customers in the United States by disguising the transactions to create the false appearance that they were unrelated to the purchase of marijuana, and thereby obtain money of, or under the custody and control, of those financial institutions and intermediaries.

(Title 18, United States Code, Section 1349.)

FORFEITURE ALLEGATION

17. As a result of committing the offense alleged in Count One of this Indictment, HAMID AKHAVAN, a/k/a "Ray Akhavan," and RUBEN WEIGAND, the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(A), any and all property constituting, or derived from, proceeds obtained directly or indirectly, as a result of the commission of said offense, including but not limited to a sum of money in United States currency representing

the amount of proceeds traceable to the commission of said offense.

Substitute Assets Provision

18. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third person;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be subdivided without difficulty;

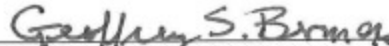
it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p) and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendants up to the value of the above forfeitable

property.

(Title 18, United States Code, Section 981;
Title 21, United States Code, Section 853; and
Title 28, United States Code, Section 2461.)



Foreperson



GEOFFREY S. BERMAN
United States Attorney
Southern District of New York

Form No. USA-33s-274 (Ed. 9-25-58)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

HAMID AKHAVAN, a/k/a "Ray Akhavan," and
RUBEN WEIGAND,

Defendants.

SEALED INDICTMENT

S3 20 Cr. 188

(18 U.S.C. § 1349.)

GEOFFREY S. BERMAN
United States Attorney.

A TRUE BILL

 3/9/20

Foreperson.
